

The Asymptotic Distribution of Exponential Sums, II

S. J. Patterson

CONTENTS

- 1. Introduction
- 2. The Conjecture
- 3. An Integral Representation
- 4. The Numerical Evidence
- 5. The Genesis of the Conjecture
- 6. On Theorem 2.1
- Acknowledgments
- References

Let $f(x)$ be a polynomial with integral coefficients and let, for $c > 0$, $S(f(x), c) = \sum_{j \pmod{c}} \exp(2\pi i \frac{f(j)}{c})$. If f is a cubic polynomial then it is expected that $\sum_{c \leq X} S(f(x), c) \sim k(f)X^{4/3}$. In this paper, we consider the special case $f(x) = Ax^3 + Bx$ and propose a precise formula for $k(f)$. This conjecture represents a refined version of the classical Kummer conjecture.

1. INTRODUCTION

In the first paper of this series, we presented some conjectures about the asymptotics of $\sum_{c \leq X} S(f(x), c)$ where, with $f(x) \in \mathbb{Z}[x]$ and $e(y) = \exp(2\pi iy)$, we set

$$S(f(x), c) = \sum_{0 \leq j < c} e\left(\frac{f(j)}{c}\right).$$

In particular, if $\deg f = 3$ we postulated that

$$\sum_{c \leq X} S(f(x), c) \sim k(f)X^{\frac{4}{3}}$$

as $X \rightarrow \infty$. The constant was not determined but we expressed the expectation that, in this case, $\operatorname{Re}(k(f)) > 0$ and $\operatorname{Im}(k(f)) = 0$.

In this paper, we study the case $f(x) = Ax^3 + Bx$ in detail and conjecture a precise formula for $k(A, B) = k(Ax^3 + Bx)$. In the case $B = 0$, it is actually possible to prove an asymptotic formula (see [Patterson 02]). Unfortunately the experimental investigations we describe here reveal a computational error in that paper and in this paper we shall correct it. Although the expectation $\operatorname{Re}(k(f)) > 0$ of [Patterson 03] is often fulfilled, more extensive calculations have shown that it is not justified in full generality. The computations described here have become more extensive as the hardware available to the author has become more powerful.

The conjectures of this paper are based on computations that cover $X \leq 100,000$, $|B| \leq 1,001$, and A in the range $1 \leq A \leq 12$ and $A = 16, 25, 27, 32, 49, 64, 81, 121, 125, 128$. For any given value of A , all values of B were

2000 AMS Subject Classification: 11L05

Keywords: Cubic exponential sums, Kummer conjecture, Gauss sums

computed simultaneously and took about 7 days computing time with a 1.6-GHz machine. The prime powers up to 128 were needed to clarify a number of points; and all were necessary to clarify aspects of the conjecture. With slower machines the time needed increases, putting a practical limit on what is feasible. Since the method employed was to study the Fourier transform of $k(A, B)$ as a function of B , it was necessary to use a large range of B .

Since $Ax^3 + Bx$ is odd, $k(A, B)$ is real. As we indicated above, we found that, according to the conjecture, it is possible that $k(A, B) = 0$ and $k(A, B) < 0$; the first example occurs when $A = 8$ and B is odd; the second example occurs when $A = 16$ and B is odd. The conjectures of this paper not only indicate how the conjectures of [Patterson 03] have to be modified but also why it is frequently the case that the positivity conjectured in [Patterson 03] holds.

2. THE CONJECTURE

Before we discuss the conjecture we shall recall the main theorem of [Patterson 02] in its corrected version.

Theorem 2.1. *For $A \in \mathbb{Z}, A \neq 0$ there is a constant $k(A)$ so that, for $\varepsilon > 0$,*

$$\sum_{c \leq X} S(Ax^3, c) = k(A)X^{\frac{4}{3}} + \mathcal{O}(X^{\frac{5}{4} + \varepsilon})$$

with

$$k(A) = \frac{1}{4(2\pi)^{-\frac{2}{3}}\Gamma(\frac{2}{3})L(2, (\frac{-3}{*}))} \cdot \frac{\pi}{3\sqrt{3}} \cdot A^{-\frac{1}{3}} \cdot \prod_{p^k \parallel A} T_p(p^k)$$

where

$$\begin{aligned} T_p(p^k) &= \frac{p^{\lfloor k/3 \rfloor + p^{\lfloor (k-1)/3 \rfloor}}}{1+p^{-1}} \\ &\quad \text{if } k \geq 1, p \equiv 1 \pmod{3} \\ &= (p^{\lfloor k/3 \rfloor} + p^{\lfloor (k-1)/3 \rfloor}) \frac{1+p^{-1}}{1+p^{-2}} - \frac{2p^{-1}}{1+p^{-2}} \\ &\quad \text{if } k \geq 1, p \equiv 2 \pmod{3} \\ &= 3^{\lfloor \frac{k}{3} \rfloor} + 3^{\lfloor \frac{k-1}{3} \rfloor} - \frac{1}{3} \\ &\quad \text{if } k \geq 1, p = 3. \end{aligned}$$

The modification occurs in the case $p \equiv 1 \pmod{3}$. In the version in [Patterson 02], reproduced in [Patterson 03], the value of $T_p(p^k)$ was given as $p^{\lfloor k/3 \rfloor} + p^{\lfloor (k-1)/3 \rfloor} - p^{-1}$. For $k = 1$, this means that the old factor was $2 - p^{-1}$, whereas in the new version it is $\frac{2}{1+p^{-1}}$.

In the case of the smallest relevant prime $p = 7$, where $\frac{13}{7} = 1.8571\dots$ has to be replaced by $\frac{7}{4} = 1.75$, the difference is of the same order of magnitude as the “experimental errors” of the values estimated from the numerical data quoted in [Patterson 02, page 727]; the new formula fits somewhat better with experiment.

Note that we have also made use of the gamma function properties to reformulate the constant. It is also significant for our purposes that $\frac{\pi}{3\sqrt{3}} = L(1, (\frac{-3}{*}))$.

To formulate the conjecture we also need the Ramanujan sums; for clarity we shall write these as

$$c(a, b) = \sum_{\substack{x \pmod{b} \\ (x, b) = 1}} e\left(\frac{ax}{b}\right).$$

This can easily be given in “finite form” but it will generally be more illuminating for us to use this definition. We recall that this function is multiplicative in the second variable and that when $p \nmid A_o$

$$\begin{aligned} c(p^a A_o, p^d) &= \varphi(p^d) && \text{if } a \geq d \\ &= -p^{d-1} && \text{if } a = d - 1 \\ &= 0 && \text{otherwise,} \end{aligned}$$

where, as usual, φ denotes the Euler totient function.

We shall denote, as usual, the Hilbert symbol at p (a prime or ∞) by $(\cdot, \cdot)_p$.

Conjecture 2.2. *For $A \in \mathbb{Z}, A \neq 0$ there is a constant $k(A, B)$ so that*

$$\sum_{c \leq X} S(Ax^3 + Bx, c) \sim k(A, B)X^{\frac{4}{3}}$$

with

$$k(A, B) = \frac{1}{4(2\pi)^{-\frac{2}{3}}\Gamma(\frac{2}{3})L(2, (\frac{-3}{*}))} \cdot A^{-\frac{1}{3}} \cdot \prod_{p \mid 3AB} T_p(A, B),$$

where if $p \nmid A_o B_o$

$$\begin{aligned} T_p(p^a A_o, p^b B_o) &= \frac{1}{1 - \frac{1}{p^2} (\frac{-3}{p})} \left\{ \sum_{0 \leq 3j \leq a} c(p^b B_o, p^j) \right. \\ &+ \sum_{\substack{[a/3] < j < a \\ j \equiv a \pmod{2}}} c(p^b A_o B_o, p^j) p^{\frac{a-3j}{2}} \\ &+ \sum_{\substack{[a/3] < j < a \\ j \equiv a+1 \pmod{2}}} \sum_{x \pmod{p^j}} \left(\frac{x}{p}\right) e\left(\frac{p^b A_o B_o x}{p^j}\right) p^{\frac{a-3j}{2}} \\ &+ \left. \sum_{a \leq j} c(p^b B_o, p^j) \left(\frac{-3}{p}\right)^{a-j} p^{a-2j} \right\} \\ &\text{if } p \neq 2, 3 \end{aligned}$$

$$\begin{aligned}
 &= \sum_{0 \leq 3j \leq a} c(3^b B_o, 3^j) + \sum_{\substack{[a/3] < j \leq a \\ j \equiv a \pmod{2}}} c(3^b A_o B_o, 3^j) 3^{\frac{a-3j}{2}} \\
 &+ \sum_{\substack{[a/3] < j < a \\ j \equiv a+1 \pmod{2}}} \sum_{x \pmod{3^j}} \left(\frac{x}{3}\right) e\left(\frac{3^b A_o B_o x}{3^j}\right) 3^{\frac{a-3j}{2}} \\
 &+ \sum_{a < j} \sum_{x \pmod{3^j}} \left(\frac{x}{3}\right) e\left(\frac{3^b A_o B_o x}{3^j}\right) 3^{a-2j} \sqrt{3} i \\
 &\text{if } p = 3
 \end{aligned}$$

$$\begin{aligned}
 &= \frac{1}{1 - \frac{1}{4}} \left\{ \sum_{0 \leq 3j \leq a} c(2^b B_o, 2^j) \right. \\
 &+ \sum_{\substack{[\frac{a+1}{3}] < j < a \\ j \equiv a \pmod{2}}} c(2^b B_o, 2^j) 2^{\frac{a-3j}{2}} \\
 &+ \sum_{\substack{[\frac{a+1}{3}] < j < a \\ j \equiv a \pmod{2}}} \sum_{\substack{x \pmod{2^j} \\ 2 \nmid x}} e\left(\frac{2^b A_o B_o x}{2^j}\right) e(x/4) 2^{\frac{a-3j}{2}} \\
 &+ \sum_{\substack{[\frac{a+1}{3}] < j < a-1 \\ j \equiv a-1 \pmod{2}}} \sum_{\substack{x \pmod{2^j} \\ 2 \nmid x}} e\left(\frac{2^b A_o B_o x}{2^j}\right) e(x/8) 2^{\frac{a-3j+1}{2}} \\
 &+ \left. \sum_{a \leq j} c(2^b B_o, 2^j) (-3, 2)_2^{a-j} 2^{a-2j} \right\} \\
 &\text{if } p = 2.
 \end{aligned}$$

The sums appearing in the conjecture are—for fixed a, b —finite and can be easily calculated; we shall give the values below. Note that the function $T_p(A, B)$ is normalized so that if $p \nmid 3AB$ then $T_p(A, B) = 1$ and we could represent the product as being over all primes. Also, it would be natural to multiply $T_p(A, B)$ by $\left(1 - \left(\frac{-3}{p}\right) \frac{1}{p^2}\right)$ and to remove the the term $L(2, \left(\frac{-3}{*}\right))$ from the definition of the constant. For the moment, the formulation above is more convenient. In the last term of the conjecture we have written $(-3, 2)_2$ rather than -1 for conceptual clarity.

It should be emphasized that, whereas for small a there is reasonably good evidence for the conjecture, as will be discussed below, this is not so for large a . The number of computations where a is large is quite small. Moreover, the two cases where there is more extensive evidence, namely A being a power of 2 or 3, are somewhat special. Even so, in the case $p = 3$ the evidence

comes from the cases $a \leq 4$ and in the case $p = 2$, from $a \leq 7$. Beyond these, one has only the single, third power 125. Therefore, the aspects of the conjecture pertaining to large a are based to a large part on intuition and on some questionable æsthetics and should be treated with the corresponding skepticism.

As we have indicated above, one can express the individual terms as “finite” expressions. If $p \neq 2$, there are four terms in the definition of $T_p(A, B)$ and, if $p = 2$, five. There is no difficulty in combining the first, second, and last terms. If $p \neq 2, 3$ these terms contribute the following to $T(p^a A_o, p^b B_o)$:

$$\left\{ \begin{array}{ll} 1 & \text{if } a = 0, b = 0, \\ 0 & \text{if } a \geq 3, b < [\frac{a}{3}], \\ \left(1 - \frac{1}{p^2} \left(\frac{-3}{p}\right)\right)^{-1} \left(p^{[\frac{a}{3}]} + p^{[\frac{a-1}{3}]} - p^{\frac{a-b}{2}}\right) & \text{if } [\frac{a}{3}] \leq b < a-1, b \equiv a \pmod{2}, \\ \left(1 - \frac{1}{p^2} \left(\frac{-3}{p}\right)\right)^{-1} \left(p^{[\frac{a}{3}]} + p^{[\frac{a-1}{3}]} - p^{\frac{a-b-1}{2}} - p^{\frac{a-b-3}{2}}\right) & \text{if } [\frac{a}{3}] \leq b < a-1, b \equiv a-1 \pmod{2}, \\ \left(1 - \frac{1}{p} \left(\frac{-3}{p}\right)\right)^{-1} \left(T_p(p^a A_o) - \left(\frac{1}{p} \left(\frac{-3}{p}\right)\right)^{b-a+1}\right) & \text{if } b \geq a-1. \end{array} \right. \tag{2-1}$$

It was in verifying the last identity in (2-1) that the error in the calculation of T_p became evident. For $p \neq 2, 3$ the contribution from the third term is

$$\left(\frac{-A_o B_o}{p}\right) p^{\frac{a-b-2}{2}}$$

when $1 \leq \frac{a-b}{2} \leq [\frac{a+1}{3}]$ and $b \equiv a \pmod{2}$, and zero otherwise. When $p = 2$, the contribution from the third term is

$$2^{\frac{a-b}{2}-2} (-1, -A_o B_o)_2$$

if $1 < \frac{a-b}{2} \leq [\frac{a+2}{3}]$ and $a \equiv b \pmod{2}$, and zero otherwise; and the contribution from the fourth term is

$$2^{\frac{a-b}{2}-3} \{(2, -A_o B_o)_2 + (-2, -A_o B_o)_2\}$$

if $2 < \frac{a-b}{2} \leq [\frac{a+3}{3}]$ and $a \equiv b \pmod{2}$, and zero otherwise.

When $p = 3$, the contribution from the first, second, and last terms is

$$\begin{cases} 1 & \text{if } a = 2, b = 0, \\ 0 & \text{if } a \geq 3, b < [a/3], \\ 3^{\lfloor \frac{a}{3} \rfloor} + 3^{\lfloor \frac{a-1}{3} \rfloor} - 3^{\frac{a-b}{2}} & \text{if } \lfloor \frac{a}{3} \rfloor \leq b < a, \\ & b \equiv a \pmod{3}, \\ 3^{\lfloor \frac{a}{3} \rfloor} + 3^{\lfloor \frac{a-1}{3} \rfloor} - 4 \cdot 3^{\frac{a-b-3}{2}} & \text{if } \lfloor \frac{a}{3} \rfloor \leq b < a, \\ & b \equiv a - 1 \pmod{3}, \\ T_3(3^a A_o) + \left(\frac{-A_o B_o}{3}\right) \frac{1}{3^{b-a+1}} & \text{if } b \geq a. \end{cases}$$

The contribution from the third term is $(-3, -A_o B_o)_3 3^{\frac{a-b-2}{2}}$ if $1 \leq \frac{a-b}{2} \leq \lfloor \frac{a+1}{3} \rfloor$ and $b \equiv a \pmod{2}$, and is zero otherwise.

3. AN INTEGRAL REPRESENTATION

The formulation of Conjecture 2.2 is not entirely satisfactory, because of its ad hoc nature. It is therefore incumbent upon us to reformulate it in such a form that demonstrates a “natural” derivation from the polynomial $Ax^3 + Bx$ and one which at least can be extended to more general cubic polynomials. The first remark is that, by a classical theorem of Euler, one has

$$\int_{-\infty}^{\infty} \exp(2\pi i \xi^3) d\xi = \frac{1}{2(2\pi)^{-\frac{2}{3}} \Gamma(\frac{2}{3})},$$

from which it follows that, as $X \rightarrow \infty$

$$\int_{-\infty}^{\infty} \exp\left(2\pi i \frac{A\xi^3 + B\xi}{X}\right) d\xi \sim \frac{X^{\frac{1}{3}}}{2(2\pi)^{-\frac{2}{3}} \Gamma(\frac{2}{3})} A^{-\frac{1}{3}}$$

which then gives a straightforward meaning to the “archimedean” factor in Conjecture 2.2.

To deal with the “non-archimedean” terms we make use of Weil’s integral (defined in [Weil 64, Section 14, Theorem 2])

$$G_p(a) = \int_{\mathbb{Q}_p} e_p(a\xi^2) d\xi \tag{3-1}$$

where we define e_p on \mathbb{Q}_p to be the continuous character such that $e_p(x) = e(-x)$ for all $x \in \mathbb{Z}[\frac{1}{p}] \subset \mathbb{Q}$. If we set $e_\infty = e$ then (e_v) defines a character on $\mathbb{Q}_\mathbb{A}$ trivial on \mathbb{Q} . The Haar measure on \mathbb{Q}_p is taken to be the self-dual measure with respect to e_p . The integral in Equation (3-1) is improper and there are many ways to define it; we shall understand it as

$$\lim_{R \rightarrow \infty} \int_{|\xi|_p \leq R} e_p(a\xi^2) d\xi.$$

One can give an analogous definition in the case of \mathbb{R} with e_p replaced by e ; we write $G_\infty(a)$ for this integral. Next, we define

$$\gamma_v(a) = |a|_v^{\frac{1}{2}} G_p(a)$$

where v denotes either a prime or ∞ . Thus $\gamma_v(a)$ depends on a , modulo squares. Weil [Weil 64, Section 28] showed that

$$\gamma_v(ab)\gamma_v(1) = (a, b)_v \gamma_v(a)\gamma_v(b)$$

where as before $(\cdot, \cdot)_v$ denotes the (quadratic) Hilbert symbol at v . Weil also proved the global theorem [Weil 64, Section 30]

$$\prod_v \gamma_v(a) = 1$$

for $a \in \mathbb{Q}^\times$. This represents a modern version of Gauss’ determination of the sign of the Gauss sum. One can determine the γ_v explicitly. The case $v = \infty$ is due to Euler and one has

$$\gamma_\infty(a) = \frac{1 + \text{sgn}(a)i}{2}.$$

If $p \neq 2$ is a prime then one has $\gamma_p(u) = 1$ when u satisfies $|u|_p = 1$ and $\gamma_p(p) = \epsilon_p^{-1}$, where $\epsilon_p = 1$ if $p \equiv 1 \pmod{4}$ and $\epsilon_p = i$ if $p \equiv 3 \pmod{4}$. For $p = 2$, we have $\epsilon_2(u) = 1 - i$ if $u \in \mathbb{Z}_2$ and $u \equiv 1 \pmod{4}$ and $\epsilon_2(u) = 1 + i$ if $u \equiv -1 \pmod{4}$. We also have $\gamma_2(2) = 1 - i$. Using these values we can deduce all the remaining values of γ_v .

More generally, we need the integral

$$\int_{|\xi|_p \leq R} e_p(a\xi^2) d\xi$$

where p is a prime. If $p \neq 2$ this is easy to determine; it equals R if $|a|_p R^2 \leq 1$ and equals $|a|_p^{\frac{1}{2}} \gamma_p(a)$ otherwise. If $p = 2$ then the integral is again R if $|a|_2 R^2 \leq 1$ and it is $|a|_2^{\frac{1}{2}} \gamma_2(a)$ if $|a|_2 R^2 \geq 4$. In the remaining case $|a|_2 R^2 = 2$, the integral is 0.

Now we can turn to the first integral which interests us here. We shall prove the following proposition.

Proposition 3.1. *Let $f(x) = Ax^3 + Bx$ and let p be a prime. Let $A = p^a A_o$ and $B = p^b B_o$ where A_o and B_o are p -units. Let $R = p^{-\delta}$ where $\delta \geq 0$ is an integer. Set*

$$I_p(A, B) = \int_{|u|_p=R} \int_{|x-y|_p \leq \rho} e_p \left(\frac{f(x) - f(y)}{(x-y)u} \right) dx dy du. \quad (3-2)$$

Then, if $p \neq 2, 3$ we have $I_p(A, B) =$

$$\begin{cases} \rho p^{(a-5\delta)/2} c(B, p^\delta) & \text{if } \rho^2 < p^{a-\delta}, \\ & a \equiv \delta \pmod{2} \\ \rho p^{(a-3\delta-1)/2} (p, -3A_o B_o)_p & \text{if } \rho^2 \leq p^{a-\delta}, \\ & a \equiv \delta - 1 \pmod{2}, \\ & b = \delta - 1 \\ 0 & \text{if } \rho^2 \leq p^{a-\delta}, \\ & a \equiv \delta - 1 \pmod{2}, \\ & b \neq \delta - 1 \\ p^{a-2\delta} c(B, p^\delta) \left(\frac{-3}{p} \right)^{a-\delta} & \text{if } \rho^2 \geq p^{a-\delta}. \end{cases} \quad (3-3)$$

If $p = 2$ then $I_2(A, B) =$

$$\begin{cases} \rho 2^{(a-5\delta)/2} c(B, 2^\delta) & \text{if } \rho^2 \leq 2^{a-\delta-2}, \\ & a \equiv \delta \pmod{2}, \\ & \delta \neq b + 2 \\ \rho 2^{(a-5\delta)/2} (c(B, 2^\delta) + 2^{\delta-1} (-1, -A_o B_o)_2) & \text{if } \rho^2 \leq 2^{a-\delta-2}, \\ & a \equiv \delta \pmod{2}, \\ & \delta = b + 2 \\ \rho 2^{(a-3\delta-3)/2} ((2, -A_o B_o)_2 + (-2, -A_o B_o)_2) & \text{if } \rho^2 \leq p^{a-\delta-2}, \\ & a \equiv \delta - 1 \pmod{2}, \\ & \delta = b + 3 \\ 0 & \text{if } \rho^2 \leq 2^{a-\delta-2}, \\ & a \equiv \delta - 1 \pmod{2}, \\ & \delta \neq b + 3 \\ 0 & \text{if } \rho^2 = 2^{a-\delta-1} \\ 2^{a-2\delta} c(B, 2^\delta) (-1)^{a-\delta} & \text{if } \rho^2 \geq 2^{a-\delta}. \end{cases} \quad (3-4)$$

If $p = 3$ then $I_3(A, B) =$

$$\begin{cases} \rho 3^{(a-5\delta)/2} c(B, p^\delta) & \text{if } \rho^2 \leq 3^{a-\delta}, \\ & a \equiv \delta - 1 \pmod{2} \\ \rho 3^{(a-3\delta)/2} (3, -3A_o B_o)_p & \text{if } \rho^2 \leq 3^{a-\delta}, \\ & a \equiv \delta \pmod{2}, \\ & b = \delta - 1 \\ 0 & \text{if } \rho^2 \leq 3^{a-\delta}, \\ & a \equiv \delta \pmod{2}, \\ & b \neq \delta - 1 \\ 3^{a-2\delta} (-3, -A_o B_o)_3 & \text{if } \rho^2 > 3^{a-\delta}, \\ & b = \delta - 1 \\ 0 & \text{if } \rho^2 > 3^{a-\delta}, \\ & b \neq \delta - 1. \end{cases} \quad (3-5)$$

(3-3) *Proof:* The proof is merely a computation. Writing $x = y + h$, the integral in Equation (3-2) becomes

$$\int_{|u|_p=R} \int_{|h|_p \leq \rho} \int e_p \left(\frac{3Ay^2 + 3Ayh + Ah^2 + B}{u} \right) dy dh du.$$

By completing the square we can evaluate the integral over y :

$$\int_{|u|_p=R} \int_{|h|_p \leq \rho} e_p \left(\frac{Ah^2}{4u} + \frac{B}{u} \right) \left| \frac{3A}{u} \right|_p^{-\frac{1}{2}} \gamma_p \left(\frac{3A}{h} \right) dh du.$$

Now we can compute the integral over h . This yields

$$\rho \int_{|u|_p=R} e_p \left(\frac{B}{u} \right) \left| \frac{3A}{u} \right|_p^{-\frac{1}{2}} \gamma_p \left(\frac{3A}{u} \right) du, \quad (3-6)$$

if $|A/4|_p \rho^2 \leq R$,

$$\int_{|u|_p=R} \left| \frac{A}{4u} \right|_p^{-\frac{1}{2}} \gamma_p \left(\frac{A}{4u} \right) e_p \left(\frac{B}{u} \right) \left| \frac{3A}{u} \right|_p^{-\frac{1}{2}} \gamma_p \left(\frac{3A}{u} \right) du, \quad (3-7)$$

if $|A/4|_p \rho^2 \geq R|2|_p^{-2}$, and zero if $|A/4|_p \rho^2 = 2R$ when $p = 2$. When $p \neq 2$ the condition that yields Expression (3-6) is $|A|_p \rho^2 \leq R$ and Expression (3-7) is $|A|_p \rho^2 > R$. In the case $p = 2$ the condition that yields (3-6) is $|A|_p \rho^2 \leq R/4$, (3-7) is $|A|_p \rho^2 \geq R$, and zero is $|A|_p \rho^2 = R/2$.

Using the multiplicative property of γ_p we find that Expression (3-7) is

$$R|2|_p |A|_p^{-1} |3|_p^{-\frac{1}{2}} \int_{|u|_p=R} (-3, A/u)_p e_p(B/u) du \gamma_p(3) \gamma_p(1).$$

If $p \neq 3$ then this becomes

$$R^3 |A|_p^{-1} c(B, p^\delta) (-3, A/p^\delta)_p,$$

as the Hilbert symbol is trivial on p -units unless $p = 3$. When $p = 3$ the integral is a Gauss sum and therefore is zero unless $|B|_3 = 3R$. In that case it is

$$-R^2 (-3, AB)_3 |A|_3^{-1}.$$

Expression (3-6) is a little more intricate. Writing $u = p^\delta u_1^{-1}$, (3-6) becomes

$$\rho R^{\frac{3}{2}} |3A|_p^{-\frac{1}{2}} \int_{|u_1|_p=1} e_p \left(\frac{Bu_1}{p^\delta} \right) \gamma_p \left(u_1 \frac{3A}{p^\delta} \right) du_1.$$

Again using the multiplicative property of γ_p we find that this becomes

$$\begin{aligned} & \rho R^{\frac{3}{2}} |3A|_p^{-\frac{1}{2}} \times \\ & \int_{|u_1|_p=1} e_p \left(\frac{Bu_1}{p^\delta} \right) \gamma_p \left(\frac{3A}{p^\delta} \right) \gamma_p(u_1) \left(\frac{3A}{p^\delta}, u_1 \right)_p du_1. \end{aligned} \tag{3-8}$$

We consider the cases $p \neq 2$ and $p = 2$ separately.

When $p \neq 2$, it follows that $\gamma_p(u_1) = 1$ and so the integral is a Ramanujan sum if $\text{ord}_p(3A/p^\delta) \equiv 0 \pmod{2}$ and a Gauss sum if $\text{ord}_p(3A/p^\delta) \equiv 1 \pmod{2}$. In the first case Expression (3-8) reduces to

$$\rho R^{\frac{3}{2}} |3A|_p^{-\frac{1}{2}} c(B, p^\delta).$$

In the second case the integral in Expression (3-8) is zero unless $\text{ord}_p(B/p^\delta) = -1$ in which case the expression reduces to

$$(p, B_o)_p \bar{e}_p \rho R^{\frac{3}{2}} |3A|_p^{-\frac{1}{2}} p^{-\frac{1}{2}} \gamma_p(3A/p^\delta),$$

which simplifies to

$$\rho R^{\frac{3}{2}} |3A|_p^{-\frac{1}{2}} p^{-\frac{1}{2}} (p, -3A_o B_o)_p.$$

The case $p = 2$ is similar but now $\gamma_2(u_1)$ is not constant but equal to $1 - i(-1, u_1)_2$. For this reason the integral is a sum of two terms. It is convenient to first replace u_1 by $3A_o u_1$ in Expression (3-8). It becomes

$$\rho R^{\frac{3}{2}} |3A|_2^{-\frac{1}{2}} \int_{|u_1|_2=1} e_2 \left(\frac{3A_o B u_1}{2^\delta} \right) \gamma_2(u_1 2^{a-\delta}) du_1. \tag{3-9}$$

Again we treat the cases in which $\text{ord}_2(3A/2^\delta)$ is even and odd separately. In the even case (3-9) becomes

$$\rho R^{\frac{3}{2}} |3A|_2^{-\frac{1}{2}} \int e_2 \left(\frac{3A_o B u_1}{2^\delta} \right) (1 - i(-1, u_1)_2) du_1.$$

Evaluated, this consists of two terms corresponding to the two terms inside the parentheses. The second is non-zero only when $\delta = b + 2$ and is a Gauss sum which can be computed explicitly. We obtain the sum of

$$\rho R^{\frac{3}{2}} |3A|_2^{-\frac{1}{2}} c(3A_o B, 2^\delta)$$

and

$$\rho R^{\frac{3}{2}} |3A|_2^{-\frac{1}{2}} 2^{-1} (-1, 3A_o B_o)_2 \begin{cases} 1 & \text{if } \delta = b + 2 \\ 0 & \text{otherwise.} \end{cases}$$

If $\text{ord}_2(3A/2^\delta)$ is odd then (3-9) becomes

$$\rho R^{\frac{3}{2}} |3A|_2^{-\frac{1}{2}} \int e_2 \left(\frac{3A_o B u_1}{2^\delta} \right) ((2, u_1)_2 - i(-2, u_1)_2) du_1$$

and now both Hilbert symbols are characters of conductor 2^3 . This means that the value of the expression is zero unless $\delta = b + 3$. Otherwise, a calculation shows that it is

$$\rho R^{\frac{3}{2}} |3A|_2^{-\frac{1}{2}} (2\sqrt{2})^{-1} ((2, -A_o B_o)_2 + (-2, -A_o B_o)_2).$$

This completes the proof of the proposition. □

Next, we evaluate a somewhat simpler integral.

Proposition 3.2. *Let p be a prime number and let $f(x) = Ax^3 + Bx$ where A, B are p -integers. As before, let $A = p^a A_o$ and $B = p^b B_o$ where A_o and B_o are p -adic units. Then for R with $p^{-[a/3]} \leq R \leq 1$ we have*

$$\int_{|u|_p=R} \int_{|v|_p \leq 1} e_p \left(\frac{f(uv)}{v} \right) dv du = \int_{|u|_p=R} e_p(Bu) du$$

and for $p \neq 2$ and R with $p^{-a} \leq R < p^{-[a/3]}$ we have

$$\begin{aligned} & \int_{|u|_p=R} \int_{|v|_p \leq 1} e_p \left(\frac{f(uv)}{v} \right) dv du = \\ & |3|_p^{\frac{1}{2}} R^{-1} \int_{|u|_p=R} \int_{|x-y|_p \leq 1} e_p \left(\frac{f(x) - f(y)}{(x-y)u} \right) dx dy du. \end{aligned} \tag{3-10}$$

If $p = 2$, Equation (3-10) also holds except when $R^3 = 2|A|_2$, when the left-hand side is zero, and when $2|A|_p = R$. In the last case, the right-hand side is zero and the integral on the left-hand side is

$$2^{-a} ((2, -A_o B_o)_2 + (-2, -A_o B_o)_2)$$

if $b = a - 4$ and is zero otherwise.

Proof: We have

$$\int_{|u|_p=R} \int_{|v| \leq 1} e_p\left(\frac{f(uv)}{v}\right) dvdu = \int_{|u|_p=R} \int_{|v| \leq 1} e_p(Av^2u^3 + Bu)dvdu$$

and the evaluation of the first integral is straightforward. If $|Au^3|_p > 1$ there are two cases. First, if $p = 2$ and $\text{ord}(Au^3) = -1$ then the integral over v is zero, as we noted above. In all other cases it is $\gamma_p(Au^3)|Au^3|_p^{-\frac{1}{2}}$. We now only have to compare this with the corresponding formulæ, especially Expression (3–6) in the proof of Proposition 3.1. The assertion of the proposition now follows. \square

We can now express $T_p(p^a A_o, p^b B_o)$ in terms of these integrals by a straightforward comparison of the formulæ of this and of the previous section. We have that $T_p(p^a A_o, p^b B_o) \left(1 - \left(\frac{-3}{p}\right) \frac{1}{p^2}\right)$ is the sum of

$$\int_{1 \geq |u|_p > R} \int_{|v| \leq 1} e_p\left(\frac{f(uv)}{v}\right) \frac{dvdu}{|u|_p}$$

and

$$\int_{|u|_p \leq R} \int \int_{|x-y|_p \leq \rho} e_p\left(\frac{f(x) - f(y)}{(x-y)u}\right) \frac{dx dy du}{|u|_p},$$

where R is taken to satisfy $|A|_p^{1/3} \geq R > |A/2|_p$; if there is such an R , i.e., except in the cases $a = 0$ or $p = 2$ and $a = 0, 1$ when we take $R = 1$.

This formula is not entirely satisfactory because of the parameter R . It demonstrates that there is a formula in terms of the polynomial $f(x)$ which is invariant under the transformation $f \mapsto f^*$ where $f^*(x) = f(\theta x)$ and θ is a p -adic unit. One should also expect that the formula would be invariant under addition of a constant to f ; this is true of the second term but not of the first. For this reason we expect that there is a modification of the second integral that has this property.

4. THE NUMERICAL EVIDENCE

Conjecture 2.2 is based on computations of $k(A, B)$ via the estimate

$$X^{-\frac{4}{3}} \sum_{c \leq X} S(Ax^3 + Bx, c)$$

for $X = 10^5$ and $A \leq 12$ and $A = 16, 25, 27, 32, 49, 64, 81, 121, 125, 128$. In fact the estimate was sampled

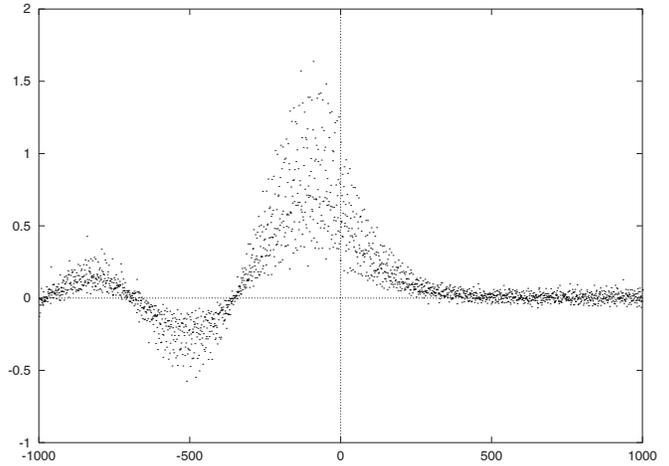


FIGURE 1. Estimations for $k(1, B)$ at $X = 10,000$.

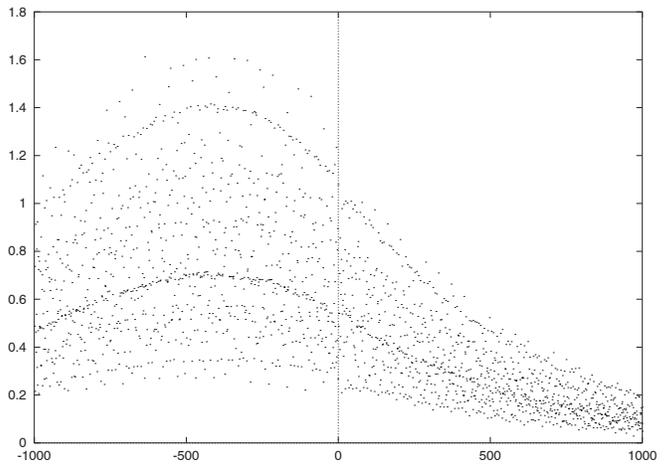


FIGURE 2. Estimations for $k(1, B)$ at $X = 100,000$.

at $X \equiv 0 \pmod{500}$. The estimates of the individual $k(A, B)$ are not very accurate, as the analysis in [Patterson 03] shows. It does not seem possible, from the data sampled, to derive a better estimate unless one knows a great deal more about the distribution a priori.

There is another problem which arises. If we examine the estimated values of $k(A, B)$ for “small” values of X , say $X = 10^4$, then we see that there is a significant “archimedean” component—see Figures 1 and 2.

In these plots one perceives lines running through the ensemble of points. These indicate that certain congruence classes modulo, for example, 6 behave in a similar fashion. Thus, for example, in the case $A = 1$, one notices that the classes with $B \equiv 5 \pmod{6}$ are especially large. This phenomenon was the first indication that a formula of the type proposed here could hold.

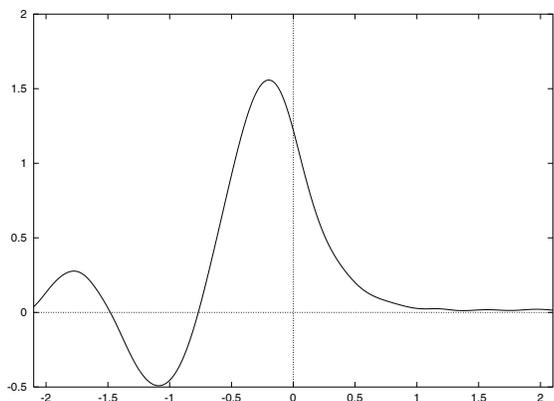


FIGURE 3. The function Φ_A for $A = 1$.

It seems to be the case that there exists a function Φ_A on \mathbb{R} so that

$$\sum_{c \leq X} S(Ax^3 + Bx, c) \sim k(A, B)X^{\frac{4}{3}}\Phi_A(B/X^{\frac{2}{3}})$$

with $\Phi_A(0) = 1$. It appears the $\Phi_A(x)$ is oscillatory when $x < 0$ and exponentially decreasing when $x > 0$. Granted that this function really exists, one can use the conjecture to tabulate it. The immediate results are very irregular but after smoothing we get a function of the type shown in Figure 3. This sort of behaviour is similar to that of certain functions associated with Bessel functions, for example, the Airy function (see, for example, [Copson 65, Chapter 9]). In our case, the function has maxima at about -0.20 and -1.76 , a minimum at -1.07 , and zeros at -0.76 , -1.47 , and -2.16 . Although their values are very approximate they suffice to rule out any of the functions one frequently encounters. One is also tempted to describe a dependence on A but it seems from the evidence—which is patchy where it is most needed—that there is no simple relationship between the different Φ_A .

It is perhaps worth noting that, whereas this sort of behaviour is in general unusual in the asymptotics of arithmetic functions, it does occur in the asymptotics of Kloosterman sums (see [Motohashi 97, Theorem 2.3 (page 64) and Theorem 2.5 (page 72)]). In [Livné and Patterson 02], we proved the existence of an asymptotic distribution of cubic exponential sums over $\mathbb{Z}[\omega]$ by exploiting an interpretation of them due to Duke and Iwaniec as “metaplectic Kloosterman sums.” The appearance of Φ_A may indicate that a similar interpretation is possible here.

For the moment the appearance of Φ_A primarily means that there are systematic errors in the estimation

of $k(A, B)$ for large $|B|$. As one has only a rudimentary understanding of Φ_A it would probably be ill-advised to attempt a correction. Also, the effects of Φ_A become smaller for large A . In any case, the “errors of measurement” for large $|B|$ and A mean that one has to treat all the data as “noisy”; for X of the order of magnitude 10^5 the effect of Φ_A is not strong, so we have assumed that it will not be serious and have ignored it.

At the outset of the calculations, the author believed that one could expect good estimates only for small values of A , say, $A \leq 10$. Yet, it turned out that for fairly large values of A , up to about 128, the convergence remained good.

In total 22 values of A were considered; for each of these, 2,003 values of $k(A, B)$ were estimated. Thus to compare the predictions of the conjecture with the measured values we would have 44,066 pairs of numbers to compare. Some are small—conjecturally zero—so it is not feasible to give quotients. The most convenient method of comparing conjecture and experiment is by plotting, for fixed A and a range of B , both the predicted and measured values which are then joined, for each B , by a line. The length of the line indicates visually how good the agreement is. In order for the lines to be visible, the maximal length of the range of B is taken to be 200. Therefore, it is only possible to present a small part of the evidence. We give a few cases ($A = 1, 2, 5, 8, 12, 32, 49, 128$) which the author hopes are convincing. Note that the role of the function Φ_A is much larger when A is small than otherwise; we illustrate this by giving the predicted and measured values when $A = 1$ for $|B| \leq 50$ (Figure 4) and $|B| \leq 100$ (Figure 5). In the first case (Figure 4), the measured value of $k(1, B)$ is denoted by an \times and the predicted value by a $+$. In the other cases (Figures 5–12), we show the line (with horizontal bars at both ends) joining the measured and predicted values, with an \times at the end denoting the measured value. One sees that this is longer when both values are large; this reflects the existence of Φ_A as a factor of proportionality. One should also note that there are effects due to “experimental errors”; for example, in the case $A = 49$ the agreement does not appear to be very good but in this case all the values are comparatively small so “experimental errors” are visually much more obvious. If B is taken in larger ranges, the effect of Φ_A is much more marked and it requires some faith to see a justification of the conjecture in the data; nevertheless one clearly sees that both experimental and predicted values are either both large or both small, and this essentially by a factor of proportionality depending only on B .

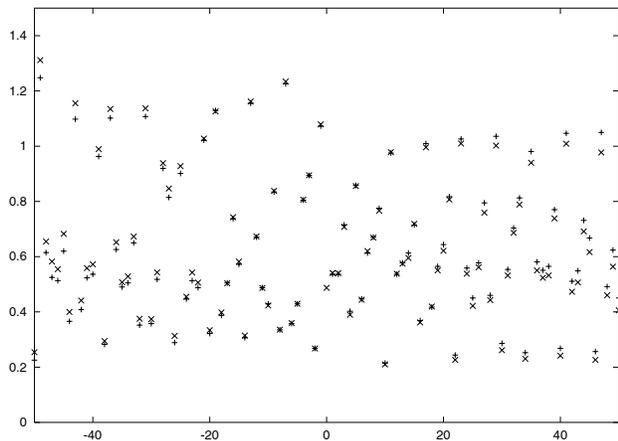


FIGURE 4. Comparison between predicted and measured values for $A = 1$ with $|B| \leq 50$.

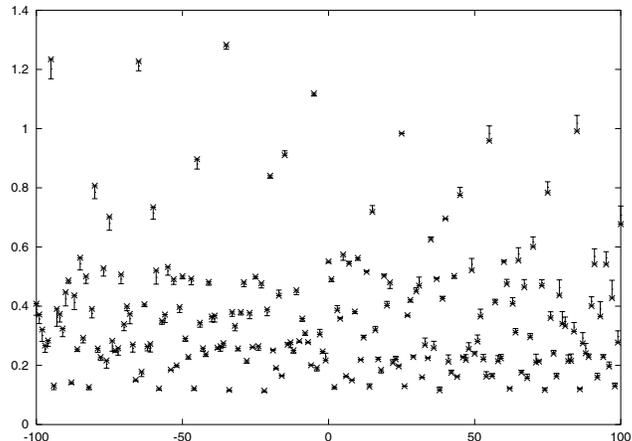


FIGURE 7. Comparison between predicted and measured values for $A = 5$.

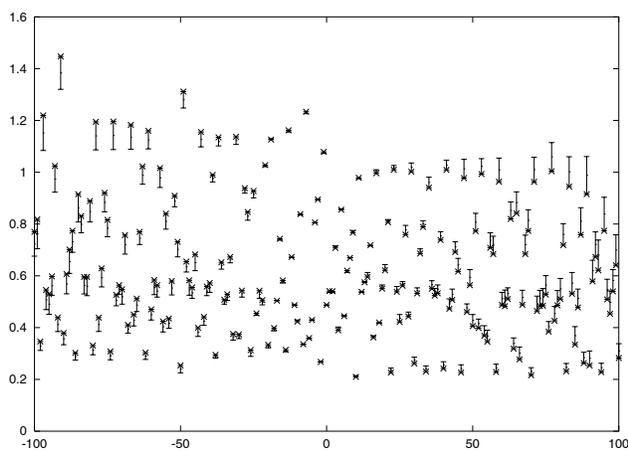


FIGURE 5. Comparison between predicted and measured values for $A = 1$ with $|B| \leq 100$.

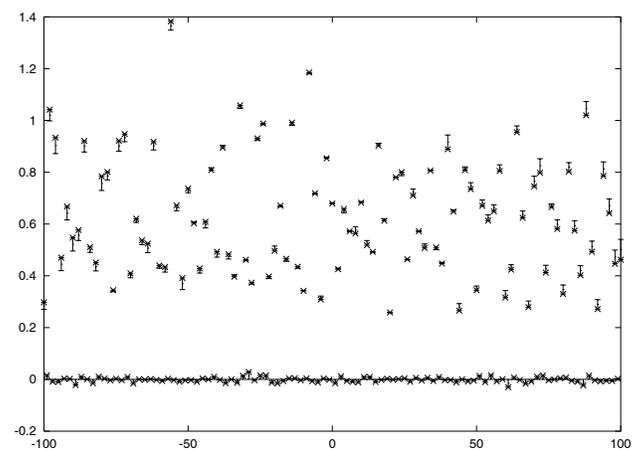


FIGURE 8. Comparison between predicted and measured values for $A = 8$.

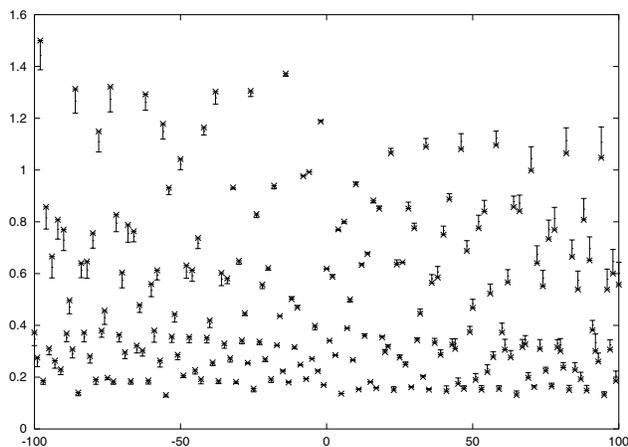


FIGURE 6. Comparison between predicted and measured values for $A = 2$.

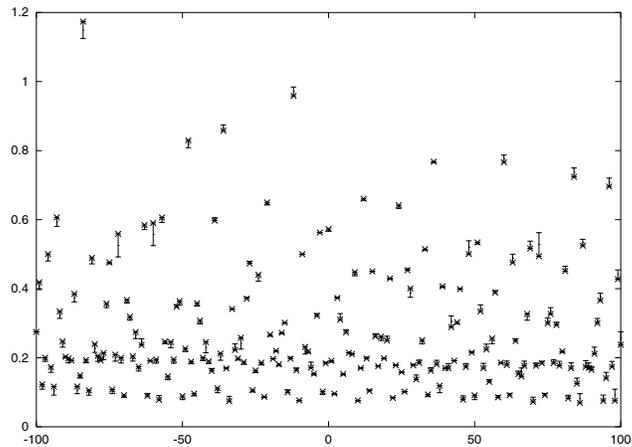


FIGURE 9. Comparison between predicted and measured values for $A = 12$.

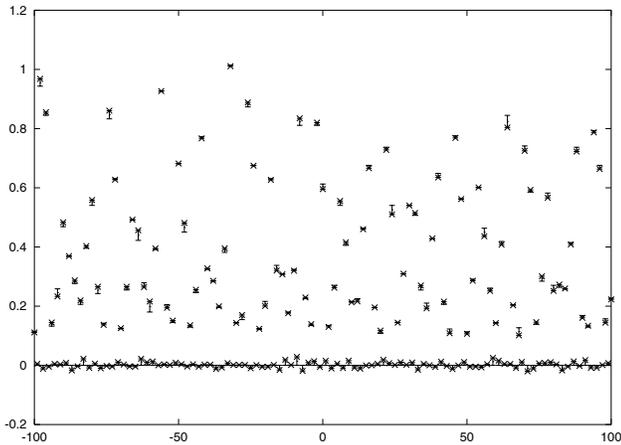


FIGURE 10. Comparison between predicted and measured values for $A = 32$.

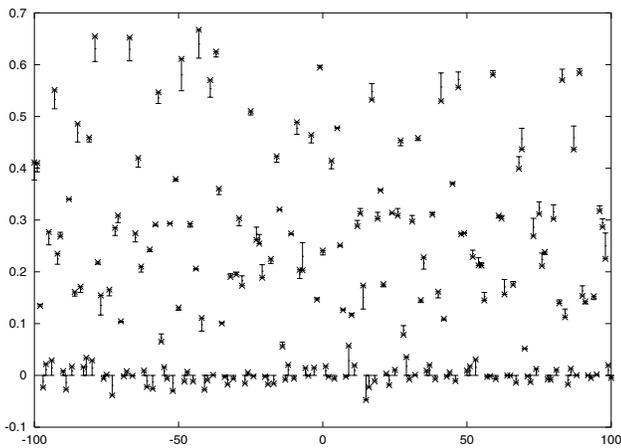


FIGURE 11. Comparison between predicted and measured values for $A = 49$.

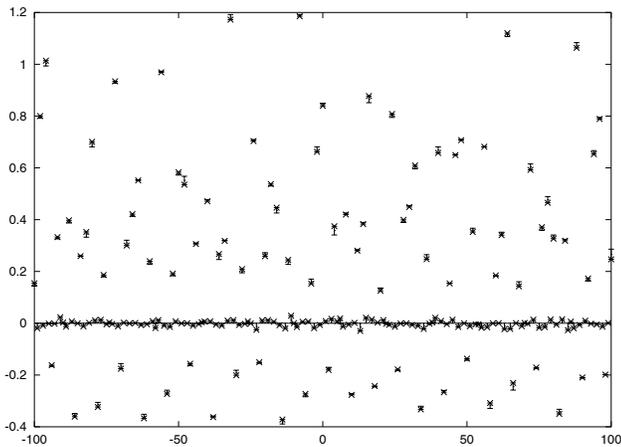


FIGURE 12. Comparison between predicted and measured values for $A = 128$.

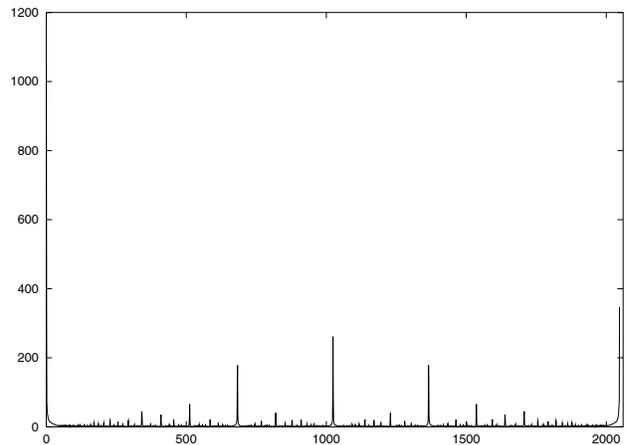


FIGURE 13. The Fourier transform (amplitude) of $k(1, B)$.

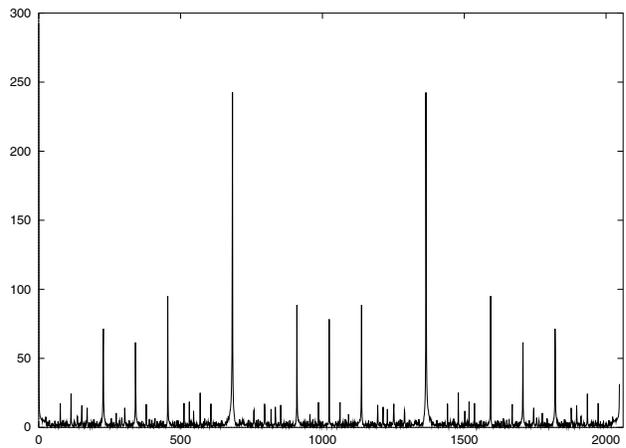


FIGURE 14. The Fourier transform (amplitude) of $k(81, B)$.

5. THE GENESIS OF THE CONJECTURE

It is clear that one could not uncover a conjecture as complex as Conjecture 2.2 directly. The vital clue as to the nature of the coefficients $k(A, B)$ came from looking at the Fourier transform of $B \mapsto k(A, B)$. The amplitude of this Fourier transform when $A = 1$ is shown in Figure 13; other values of A give similar results; we give also, as an example, $A = 81$ in Figure 14.

One recognizes at once a Farey series and the structure is familiar from the Hardy-Littlewood method. Given this, one can compute the “Fourier coefficients”

$$\hat{k}\left(A, \frac{a}{c}\right) = \frac{1}{2003} \sum_{|B| \leq 1001} e^{-2\pi i B \frac{a}{c}} k(A, B).$$

Fortunately, it turns out that $\hat{k}(A, 0) \neq 0$ and one then recognizes the $\hat{k}(A, \frac{a}{c})/\hat{k}(A, 0)$ as rational numbers or as quadratic irrationalities. The formalized version of these observations is the second version of the conjecture given at the end of Section 2 This represents a reconstruction from the data given by $\hat{k}(A, \frac{a}{c})$. It is not clear that such a reconstruction will be successful. The values of $k(A, B)$ for positive and negative B are conjecturally essentially the Fourier coefficients of an Eisenstein series of weight 2. The Fourier coefficients of a cusp form would be zero and therefore invisible. It is not entirely clear that this does not happen; for the moment the evidence seems to be that there are no cusp forms. For the general theory of arithmetic functions from a view pertinent to these considerations, see [Schwarz and Spilker 94].

Given the arithmetical nature of $k(A, B)$ there remains the problem of deducing the constant of proportionality. This was explained in Section 2

The fact that the $k(A, B)$ appear to be intimately related to Eisenstein series, together with the existence of Φ , described in Section 4, reinforces the notion that Conjecture 2.2 can be understood, and probably proved, in the context of the theory of automorphic forms; more precisely in that of metaplectic forms as in [Livné and Patterson 02]. One may expect that an analogue of the conjecture holds for $S(f(x), c)$ for f of degree greater than three, but it is very unlikely that an interpretation of this kind exists.

6. ON THEOREM 2.1

We noted in Section 2 that the version of Theorem 2.1 given in [Patterson 02] for the case $p \equiv 1 \pmod{3}$ is flawed. The calculations in this paper indicate strongly that

$$T_p(p^a A_o) \left(1 - \left(\frac{-3}{p} \right) \frac{1}{p^2} \right) = 1 - \frac{1}{p} + \left(1 - \left(\frac{-3}{p} \right) \frac{1}{p} \right) \times \left(\sum_{0 \leq 3j \leq a} \varphi(p^j) + \sum_{\substack{a < 3j < 3a \\ j \equiv a \pmod{2}}} \varphi(p^j) p^{\frac{a-3j}{2}} \right)$$

for $p \neq 3$ and

$$T_p(3^a A_o) = 1 - \frac{1}{p} + \left(\sum_{0 \leq 3j \leq a} \varphi(p^j) + \sum_{\substack{a < 3j < 3a \\ j \equiv a \pmod{2}}} \varphi(p^j) p^{\frac{a-3j}{2}} \right)$$

for $p = 3$. This forced the author to reexamine the calculations of [Patterson 02]—particularly the part described as “laborious but entirely routine.” There are both errors and misprints in the preparations for these computations. The most serious is that a factor $\frac{1-p^{-2}}{1+p^{-2}}$ appears several times which should be $\frac{1-p^{-2}}{(1+p^{-1})^2}$ for example in the last two displayed formulæ in [Patterson 02, page 725 and page 726]. Additionally, we note that in the last displayed formula on page 725 there is a term $(1 + p^{-s})^{-1}$ which should be $(1 + p^{-2})^{-1}$. Also, in the second displayed term χ_q should be χ_9 and the exponent ± 1 not 2 ± 1 . Finally, in the third displayed formula on page 724 d_2^2 should be δ_2^2 and the exponent of $N(d_0 d_1^2)$ should be $-s$ not -3 .

With these corrections to the formulæ one can compute $T_p(p_o^a)$; the result is given in Section 2 Note that the factor $\frac{1}{1+p^{-1}} = \frac{1-p^{-1}}{1-p^{-2}}$ of $p^{[\frac{a}{3}]} + p^{[\frac{a-1}{3}]}$ is, in comparison to the factor when $p \equiv 2 \pmod{3}$, namely $\frac{1+p^{-1}}{1+p^{-2}}$, now much more natural than the factor 1.

The author regrets these errors.

ACKNOWLEDGMENTS

The project described here was inspired by R. Livné and the collaboration with him which led to [Livné and Patterson 02].

The author would also like to take this opportunity to express his thanks to the large group of programmers who have made available a wide range of tools which have been of inestimable value. These are the GNU version of the Unix programming environment, especially `gcc`, `gawk`, and also `gnuplot`, `perl`, and the Cephass library (which includes the Airy function). Most of these were used in the `djgpp`/Cygwin port to a Windows environment.

REFERENCES

- [Copson 65] E. T. Copson. *Asymptotic Expansions*. Cambridge Tracts in Mathematics, 55. Cambridge, UK: Cambridge U.P., 1965.
- [Livné and Patterson 02] R. Livné and S. J. Patterson. “The First Moment of Cubic Exponential Sums.” *Inv. Math.* 148 (2002), 79–116.
- [Motohashi 97] Y. Motohashi. *Spectral Theory of the Riemann Zeta Function*. Cambridge Tracts in Mathematics, 127. Cambridge, UK: Cambridge University Press, 1997.
- [Patterson 02] S. J. Patterson. “On the Distribution of Certain Hua Sums, II.” *Asian J. Math.* 6 (2002), 719–730.
- [Patterson 03] S. J. Patterson. “The Asymptotic Distribution of Exponential Sums, I.” *Exp. Math* 12 (2003), 135–153.
- [Schwarz and Spilker 94] W. Schwarz and J. Spilker. *Arithmetical Functions*. LMS Lecture Notes 184. Cambridge, UK: Cambridge University Press, 1994.

[Vaughan 81] R. C. Vaughan. *The Hardy-Littlewood Method*. Cambridge Tracts in Mathematics, 80. Cambridge, UK: Cambridge University Press, 1981.

[Weil 64] A. Weil. "Sur certains groupes d'opérateurs unitaires." *Acta Math.* 111 (1964), 143-211

S. J. Patterson, Mathematisches Institut, Bunsenstr. 3-5, 37073 Göttingen, Germany (sjp@uni-math.gwdg.de)

Received July 13, 2004; accepted August 25, 2004.